

Appn. No. 09/587,228
Amendment dated June 28, 2004
Reply to Office action of Mar. 26, 2004
Docket No. 6169-130

IBM Docker No. BOC9-1999-0072

REMARKS/ARGUMENTS

These remarks are made in response to the Office Action of March 26, 2004 (Office Action). As this response is timely filed within the 3-month shortened statutory period, no fee is believed due.

In paragraphs 1-5 of the Office Action, claims 1-2, 11-14, 23-26, 35-38 and 47-48 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Number 6,256,739 to Skopp, *et al.* (Skopp) in view of U.S. Patent Number 5,819,285 to Damico (Damico) [collectively referred to as Skopp-Damico]. In paragraphs 6-13 of the Office Action, claims 3-10, 15-22, 27-34, and 39-46 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Skopp-Damico in view of U.S. Patent Number 6,537,424 to Dutta (Dutta).

In the previous office action, Applicants attempted to submit an affidavit under 37 C.F.R. § 1.131 supporting the removal of Dutta as a reference. An error evidently occurred during the transmission of this document. Dutta, however, has been removed by the Examiner in the current Office Action in light of new art, as noted in the Response to Arguments section of the Office Action. Nevertheless, paragraphs 6-13 rely upon Dutta, in contradiction to the Response to Arguments section.

To resolve this apparent conflict, Applicants have enclosed affidavits under 37 C.F.R. § 1.131 supporting the removal of Dutta as a reference. The affidavits are accompanied by a copy of the Applicants' confidential invention disclosure entitled "A Method for Preventing Deep Linking into a Web Site". The confidential invention disclosure and affidavits demonstrate proof of conception for the claimed subject matter of the Applicants' invention at least as early as July 28, 1999, which predates the effective date of Dutta. Applicants further exercised due diligence from prior to the effective date of Dutta until June 6, 2000, the filing date of the instant application.

Prior to addressing the rejections on the art, a brief review of the Applicants' invention is in order. The Applicants' invention prevents access to documents through undesired deep linking, where deep linking refers to referencing Web-based content from an external Web page. Deep linking can be used to circumvent the desires of a Web content provider. According to the disclosed and claimed invention, Web access can be granted or denied based upon the source

Appl. No. 09/587,228
Amendment dated June 28, 2004
Reply to Office action of Mar. 26, 2004
Docket No. 6169-130

IBM Docket No. BOC9-1999-0072

document, where the source document is a Web page containing a hyperlink to the Web page to which user access is desired. Consequently, Applicants provide an inventive means to prevent deep linking in an anonymous fashion that is independent of the identity of a user.

For example, a Web site may be maintained through advertiser support, where advertisements appear within designated sections of a Web page, where other sections link to Web content. Other Web sites can attempt to link to the content through a different Web portal, excluding the advertisements that support the content provider.

In another example, undesired deep linking can tarnish the reputation, prestige, and/or value of a Web providers content. That is, a Web content provider may only permit authorized external agencies and/or sites from linking to and/or embedding content from its sites. For example, a real estate broker may only wish to permit its Web content to be accessed through authorized affiliates and/or by customers directly via a home portal and not by other real estate agencies, by Web crawling engines, and the like.

Turning to the rejections on the art, in paragraphs 1-5 of the Office Action, claims 1-2, 11-14, 23-26, 35-38 and 47-48 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Skopp in view of Damico. Skopp discloses a method and apparatus that includes an access control proxy that a client computer logs onto in order to be granted Internet access, as shown in FIGS. 1A, 1B, 2, 4, and 5 of Skopp. Skopp is designed as a method through which advertisers can provide free Internet access to users in a limited fashion, where the access limitations are established in a user variable manner by an Internet service provider. That is, the access control proxy is designed as a client-side mechanism for restricting Web pages that an ISP permits subscribing clients to access.

The proxy of Skopp can determine a user identity and can provide access to a limited set of Web pages based upon the user identity. All of the access control techniques detailed by Skopp are based upon user-identity, which is a typical means for securing information for the Internet.

Turning now to Damico, Damico teaches how a cooperating Web content partner can encode information about themselves when referring a customer to a partner Website. For example, if GOOGLE (TM) were to refer a customer to a partner Website, GOOGLE might do

Appl. No. 09/587,228
Amendment dated June 28, 2004
Reply to Office action of Mar. 26, 2004
Docket No. 6169-130

IBM Docket No. BOC9-1999-0072

so by linking the customer to the partner site using a link like "http://www.(partner_site).com/page-link/cgi?partner=GOOGLE." The partner site that receives the link can credit the "linking site", ignore the partner identifier, and the like. Further, a partner, like a search engine or ISP, can capture a customer's navigational history and provide it to a partner (presumably for an additional fee) so that the partner can conduct direct market solicitations based upon this navigation history or provide targeted services based upon the navigational history. Damico, is silent in regards to using the disclosed co-marketing technique as a security mechanism or as a means to prevent deep linking.

Referring to claims 1 and 25, Applicants specifically claim the steps of: (emphasis added)

establishing a list of allowable source documents from which a request to access said document can originate;
receiving a request for said document from a requesting client;
detecting in said request an identity of a source document of said request;
comparing said detected identity with said list of allowable source documents from which a request to access said document can originate; and,
servicing said request if said detected identity matches an allowable source document contained in said list of allowable source documents.

The Examiner has conceded that Skopp fails to teach using a source document as a security mechanism. The Examiner, however, asserts that Skopp otherwise "teaches the invention substantially as claimed." Applicants respectfully disagree.

Skopp teaches an access control proxy that permits an ISP to restrict target Web sites from a subscriber. The Access Control List (ACL) is a destination or target based restriction, as noted at column 6, line 65 to column 7 line 27 and at column 8, line 19 to column 9, line 27. Skopp fails to teach restricting access based on an originating source. Damico fails to cure this deficiency. Accordingly, the § 103(a) rejections as to claims 1-12 and claims 25-36 should be withdrawn, which action is respectfully requested.

Moreover, Applicants' claimed limitations that access restrictions are based upon an originating source is not taught or suggested by Skopp, Damico, nor any combination thereof. Notably, an access restriction based on a source can be implemented by a Web server, as shown in FIG. 3 of the Applicants invention.

Appl. No. 09/587,228
Amendment dated June 28, 2004
Reply to Office action of Mar. 26, 2004
Docket No. 6169-130

IBM Docker No. BOC9-1999-0072

No equivalent access restriction is possible based upon the teachings of Skopp, which fails to teach or suggest any means through which a WEB SERVER can restrict access to served Web content. Instead Skopp teaches how an ISP can restrict access granted to subscribers (based upon the destination list). That is, Skopp could be used as a means for providing access control (such as parental safeguards for children surfing the Web) but not as a means for Web servers to restrict content from content requesting entities. Damico fails to cure this deficiency.

Additionally, Skopp teaches using a standard, known access control methodology (based upon user identity) in an inventive way so that ISP's can provide Internet access in an advertiser supported fashion. Damico fails to overcome this deficiency in Skopp, in that Damico fails to teach or suggest using a Web document as an access control method.

The teachings of Damico are to be used as a means for partnered Websites to provide remuneration to a partner based upon a number of partner-linked customer accesses. Contrary to the Examiner's assertion, the column 6, lines 23-38 fails to teach an access control methodology based upon a source document.

In Damico, the OLS 140 will accept a USER that is routed by an authorized co-marketer. Before this acceptance of a user occurs, "specialized user software 106 is preferably provided to a user of a user station 102 by an on-line service co-marketer (CM) and loaded onto PC 104 prior to the time the user station 102 attempts to enroll on OLS 140," as stated at column 4, lines 62 to 66. The software loaded on the user station 102 is used to authenticate the user to the OLS 140 based presumably upon a user or user station 102 identifier. A private/public key arrangement could presumably be used as the security arrangement permitting the secured transaction. Access restrictions are based upon parameters based between the user software 102 and the enrollment server 145. Column 6, lines 23-38 describes that one parameter used by the user software 102 for authentication can include the identity of the co-marketer.

The requirement that security provided by Damico is primarily based upon user identity is emphasized in FIG. 2 of Damico. For example, FIG. 2 requires a new user associated with a user station to enroll onto OLS 140, as stated at column 7, lines 16-18. Enrollment requires a user to enter a login name and comparing the login name against a list of valid login names maintained in enrollment database 146, as noted at column 7, lines 29-34. Processing to step 220

Appl. No. 09/587,228
Amendment dated June 28, 2004
Reply to Office action of Mar. 26, 2004
Docket No. 6169-130

IBM Docket No. BOC9-1999-0072

only proceeds once a user logs in using their user identity. Accordingly, Damico fails to teach servicing said request detected identity matches an allowable source document.

Further, Applicants point out that one of ordinary skill in the art would not combine the references in the manner suggested by the Examiner to prevent deep linking. Placing embedded information within a http request (as taught by Damico to identify co-partner information) would be completely ineffective for the purposes of the Applicants' invention. That is, one would not convey information needed to authorize a link, within the link itself. Link information is conveyed in an open fashion via the Internet. Such a conveyance would provide no security. Further, when authorization information is contained within a link, a Web server would have no way of distinguishing whether the deep-link attempt originated from a legitimate link or an illegitimate one.

Applicants emphasize that Damico does not teach or suggest linking in this fashion, either. Damico establishes security via access control mechanisms based upon an enrolled user station, where enrollment identifies and authenticates a user. The co-partner identifier (passable within a link) is a means for taking a programmatic action AFTER a user has been security identified (as noted in block 220 of FIG. 2) by the OLS and logged into the OLS system.

In contrast, the Applicants use the HTTP "referrer" header to determine the source document containing the link or href that originated a request. The referrer header does provide a means for a Web server to distinguish the source of a Web request, thereby permitting a Web server to service a request if the detected identity (of a source document) matches an allowable source document, as claimed.

For the above reasons, claims 1 and 25 are not obvious based upon Skopp, Damico, and/or any combination thereof. Accordingly, Applicants respectfully request that the 35 U.S.C. § 103(a) rejections as to claims 1-12 and claims 25-36 be withdrawn.

Referring to claims 13 and 37, Applicants claim the steps of:

- establishing a list of prohibited source documents from which a request to access said document cannot originate;
- receiving a request for said document from a requesting client;
- detecting in said request an identity of a source document of said request;
- comparing said detected identity with said list of prohibited source documents from which a request to access said document cannot originate; and,

Appl. No. 09/587,228
Amendment dated June 28, 2004
Reply to Office action of Mar. 26, 2004
Docket No. 6169-130

IBM Docket No. BOC9-1999-0072

denying said request if said detected identity does matches a prohibited source document contained in said list of prohibited source documents.

Claims 13 and 37 should be allowed for the same reasons as claims 1 and 25 should be allowed. Neither Skopp, Damico, nor any combination thereof teach or suggest an access restriction methodology based upon originating document. Neither Skopp, Damico, nor any combination thereof teach or suggest a method that could be applied by a Web server, as could the method of claim 13 and 37 to provide Web content. Neither Skopp, Damico, nor any combination thereof match an identity from an incoming document to a list of prohibited Web documents. Generally, the teachings of Skopp or Damico cannot be applied by one of ordinary skill to resolve the problem of deep linking, as claimed by the Applicants. Consequently, claims 13 and 37 are not obvious based upon Skopp, Damico, and/or any combination thereof. Accordingly, Applicants respectfully request that the 35 U.S.C. § 103(a) rejections as to claims 13-24 and claims 37-48 be withdrawn.

Further still, regarding paragraphs 1-5 of the Office Action, Applicants respectfully submit that the prior art of record fails to express the desirability to combine the teachings of Skopp with the teachings of Damico in the manner suggested by the Examiner. As noted in *In re Gordon*, 733 F.2d 999, 221 USPQ at 1127 "the mere fact that prior art may be modified in the manner suggested by the Examiner does not make the modification obvious unless the prior art suggests the desirability of the modification."

Absent such a suggestion, it is improper to combine the references of Skopp and Damico. Applicants fail to see how an advertiser based ISP connectivity methodology of Skopp relates to a marketing co-partnering application of Damico other than both utilize the Internet. Additionally, Applicants fail to see how it is obvious to attempt to combine two client side methodologies to teach a server based methodology, when no teachings or suggestions to that affect are included in either Skopp or Damico. Further, Applicants fail to see the motivation to combine two methodologies that require users to log into a system and that base access at least in part upon user identity to achieve an anonymous access control system based upon Web document identity. Accordingly, claims 1-48 should be allowed based on a lack of motivation to combine the references of Skopp with Damico.

Appln. No. 09/587,228
Amendment dated June 28, 2004
Reply to Office action of Mar. 26, 2004
Docket No. 6169-130

IBM Docket No. BOC9-1999-0072


Referring to paragraphs 6-13 of the Office action, claims 3-10, claims 15-22, claims 27-34, and claims 39-46 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Skopp-Damico in view of U.S. Patent Number 6,537,424 to Dutta (Dutta). Applicants are confused as to the Examiner's reliance upon Dutta, as the Examiner has stated in the Response to Arguments that Dutta has been removed as a reference. In support of this removal, Applicants have filed a declaration under 37 CFR 1.131 as previously stated. Accordingly, rejections to claims 3-10, claims 15-22, claims 27-34, and claims 39-46 should be withdrawn, which action is respectfully requested.

Referring to paragraph 7, Applicants are unable to ascertain whether Dutta was used by the Examiner as to claims 12, 24, 36, and 48. Applicants believe that paragraph 7 of the Office Action should proceed paragraph 6 and that paragraph 8 provides support for the rejection of paragraph 6. Either way, claims 12, 24, 36, and 48 should now be in allowable condition, as each are dependent upon a claim that should be in an allowable state for reasons expressed herein.

Applicants believe that this application is now in full condition for allowance, which action is respectfully requested. Applicants request that the Examiner call the undersigned if clarification is needed on any matter within this Amendment, or if the Examiner believes a telephone interview would expedite the prosecution of the subject application to completion.

Respectfully submitted,

Date: 28 June 2004


Gregory A. Nelson, Registration No. 30,577
Kevin T. Cuenot, Registration No. 46,283
Brian K. Buchheit, Registration No. 52,667
AKERMANN SENTERFITT
Post Office Box 3188
West Palm Beach, FL 33402-3188
Telephone: (561) 653-5000